Huddly App macOS security vulnerability

CVE ID: CVE-2024-22882

CVSS Score: 7.3 - High

Workarounds: N/A

Summary

A vulnerability has been identified in the Huddly App for macOS, that allows an attacker to run malicious software disguised as the Huddly App.

Applications built with Electron can by default be run as a regular node process from the terminal on macOS. When running as a node process, it will inherit the same TCC (Transparency, Consent, and Control) permissions as the application in question. It can also gain heightened privileges by prompting the user for these all while being disguised as the original application.

This can be exploited for code injection, enabling an attacker with access to easily run malicious software on the host.

Affected products

Huddly App on macOS earlier than 3.5.10

Mitigation

Upgrade the Huddly App for macOS application to version 3.5.10 or newer from
https://www.huddly.com/software-releases/

History

Version	Date	Description
	27.12.2023	Huddly verified vulnerability
	04.04.2024	Huddly app for macOS 3.5.10 released with fix for vulnerability
1.0	04.04.2024	Vulnerability report posted